69. *Curves of Genus 2 with a Rational Torsion Divisor of Order 23*

By Hiroyuki OGAWA

Department of Mathematics, Osaka University

(Communicated by Shokichi IYANAGA, M. J. A., Nov. 14, 1994)

§1. Introduction. Flynn [1] (resp. Leprévost [6], [7]) got infinitely many curves defined over $\boldsymbol{Q}$ with a rational torsion divisor of order $N = 11$ (resp. 13, 15, 17, 19 and 21), by constructing a curve of genus 2 defined over $\boldsymbol{Q}(t)$ with a rational torsion divisor of order N. In this paper, we shall extend these results to the case of $N = 23$. We remark that Leprévost [8] gave some curves over $\boldsymbol{Q}$ with a rational torsion divisor of order 22, 23, 24, 25, 26, 27 and 29, respectively.

Many studies have been made to find algebraic curves with a large rational torsion divisur, or abelian varieties with a large rational torsion point. In case of genus 1, lots of elliptic curves with a large rational torsion were explicitly constructed, before the appearance of the universal bound of torsion of elliptic curves over $\boldsymbol{Q}$ (resp. over any quadratic number field) by Mazur [9] (resp. by Kamienny [5]). On the other hand, Gross-Rohrich [3] and Shioda [10] constructed a family of g-dimensional abelian varieties over $\boldsymbol{Q}$ with a rational torsion point of order $2g + 1$, using Fermat varieties, and Flynn [2] and Leprévost [7] gave families of hyperelliptic curves of genus g over $\boldsymbol{Q}$ with a rational torsion divisor of order $2g^2 + 2g + 1$ and $2g^2 + 3g + 1$, respectively. As for universal bounds of torsions like Mazur's, we know only the result on torsions of abelian varieties of CM-type due to Silverberg [11], who, in the 2-dimensional case over $\boldsymbol{Q}$, showed that the order of a rational torsion point is at most $185640 = 2^3 \cdot 3 \cdot 5 \cdot 7 \cdot 13 \cdot 17$.

An abelian variety without any non-trivial abelian subvarieties is called simple. Leprévost's example with a 24-torsion is not simple, by easy calculation, and those with a 25-torsion and with a 27-torsion probably not, as we can decompose their congruence zeta functions for each prime $p < 1000$. We can easily construct abelian varieties with a large torsion using the product of clliptic curves with large torsions. For example, if E and E' are two elliptic curves over $\boldsymbol{Q}$ with a rational 10-torsion and with a rational 9-torsion, respectively, then the product $E \times E'$ has a rational torsion of order $90 = 10 \times 9$. So, in search for abelian varieties with a large rational torsion, the interest would be lost without the assumption that they are simple. We remark here that the Jacobian varieties of the curves given in this paper are simple.

§2. Construction of torsion divisors with a large order. 2.1. We shall first describe briefly the method of Leprévost [6,7]. Let k be a field with $\mathrm{char}(k) \neq 2$. Let g be a positive rational integer, A a polynomial on x with

k-coefficients of degree at most g, λ a non-zero element of k such that

$$f(x) := A^2(x) - \lambda x^{g+1}(x-1)^g$$

has no multiple roots, and C the hyperelliptic curve of genus g defined over k by $y^2 = f(x)$. Since the degree of f is odd, C has only one point at infinity, that is denoted by ∞. Put $P_0 = (0, A(0))$, $P_1 = (1, A(1))$, $\mathfrak{D}_0 = P_0 - \infty$ and $\mathfrak{D}_1 = P_1 - \infty$. We see that ∞, P_0 and P_1 are rational points of C, and $\mathfrak{D}_0$ and $\mathfrak{D}_1$ rational divisors of C that are linearly inequivalent to 0.

Lemma 1 ([7]). *Suppose that there exist two rational integers a and b such that $a\mathfrak{D}_0 + b\mathfrak{D}_1 \sim 0$. Then $((g+1)b - ga)\mathfrak{D}_0 \sim 0$.*

Let $k = \boldsymbol{Q}(t)$ and $g = 2$. For each $l = 15, 17, 19$ and 21, Leprévost found A, λ, a and b satisfying $a\mathfrak{D}_0 + b\mathfrak{D}_1 \sim 0$ and $3b - 2a = l$, respectively, and, by Lemma 1, obtained that

Theorem 2 ([7]). *There exist curves of genus 2 defined over $\boldsymbol{Q}(t)$ with a rational torsion divisor of order 15, 17, 19 and 21, respectively.*

Corollary ([7]). *There exist infinitely many curves of genus 2 over $\boldsymbol{Q}$ with a rational torsion divisor of order 15, 17, 19 and 21, respectively.*

2.2. We modify the above method for our aim. Let k, g and A be as above, λ a non-zero element of k such that

$$f(x) := A^2(x) - \lambda x^{g+2}(x-1)^{g-1}$$

has no multiple roots, C the hyperelliptic curve of genus g defined over k by $y^2 = f(x)$, and ∞, P_0, P_1, $\mathfrak{D}_0$ and $\mathfrak{D}_1$ as above.

Lemma 3. *Suppose that there exist two rational integers a and b such that $a\mathfrak{D}_0 + b\mathfrak{D}_1 \sim 0$. Then $((g+2)b - (g-1)a)\mathfrak{D}_0 \sim 0$.*

The proof of the last lemma is easy and similar to that of Lemma 1. We shall find in the next section A and λ satisfying the assumption of the last lemma with $k = \boldsymbol{Q}(t)$, $g = 2$, $a = -3$ and $b = 5$ $(23 = 4 \cdot 5 - 1(-3))$, which will lead to our main result:

Theorem 4. *There exists a curve of genus 2 defined over $\boldsymbol{Q}(t)$ with a rational torsion divisor of order 23.*

It follows from the computation of Igusa's absolute invariants [4] of the curve that

Corollary. *There exist infinitely many curves of genus 2 over $\boldsymbol{Q}$ with a rational torsion divisor of order 23.*

§3. Proof of Theorem 4. We use the same notation as in 2.2, and put $k = \boldsymbol{Q}(t)$, $g = 2$ and $P_0' = (0, -A(0))$. If ϕ is a function on C with

$$(\#) \qquad \operatorname{div}(\phi) = 3P_0' + 5P_1 - 8\infty,$$

then we have that $-3\mathfrak{D}_0 + 5\mathfrak{D}_1 = \operatorname{div}(\phi/x^3) \sim 0$, hence, by Lemma 3, the hyperelliptic curve C has a rational torsion divisor of order $4\cdot 5 - (-3) = 23$. Since the vector space $L(8\infty)$ is spanned over k by $\{1, x, x^2, x^3, x^4, y, xy\}$, we may put $\phi = v - uy$, where u and v are polynomials on x of degree at most 1 and 4, respectively, and we should have

$$v^2 - u^2 f(x) = \kappa x^3(x-1)^5,$$

for some $\kappa \in k$. Comparing leading terms of the both sides, we may put v a monic polynomial and $\kappa = 1$.

$$v^2 - u^2A^2 = x^3(x-1)^5 - \lambda x^4(x-1)u^2.$$

$$\{v-uA\}\{v+uA\}=x^3(x-1)\{(x-1)^4-\lambda xu^2\}.$$

On the other hand, $\phi(P_0)\neq 0$, $\phi(P_0')=0$ and $\phi(P_1)=0$ lead to

$$x\nmid v-uA,\ x\mid v+uA \text{ and } x-1\mid v-uA,$$

respectively. Hence we can write

$$v+uA=x^3p,\ v-uA=(x-1)q,\ pq=(x-1)^4-\lambda xu^2,$$

where $p=x-\alpha$ and $u=\mu(x-\beta)$ for some $\alpha,\beta,\mu\in\boldsymbol{Q}(t)$. Hence

$$A=\frac{x^3p-(x-1)q}{2u}.$$

Since the right hand side has to be a polynomial on x, we should have

$$\begin{cases}(\alpha-1)^4-\alpha\lambda\mu^2(\alpha-\beta)^2=0\\ \beta^3(\beta-\alpha)^2-(\beta-1)^5=0.\end{cases}$$

This system of simultaneous equations is solved by

$$\alpha=\frac{t^4+10t^2+5}{2(t+1)^3},$$

$$\beta=\frac{(t+1)^2}{4t},$$

$$\lambda\mu^2=\frac{t^2(t^2+3)^4}{(t-1)^2(t+1)^3(t^4+10t^2+5)}.$$

We have a form of $\phi=v-uy$ satisfying (♯), for an arbitrary μ. This concludes the constructive proof of Theorem 4.

Putting in particular

$$\mu=\frac{t(t+1)}{2(t-1)^2(t^4+10t^2+5)},$$

and substituting $(t+1)^2x$ on x, for simplicity, we obtain

$$f(x)=A^2(x)-\lambda x^4((t+1)^2x-1),$$

where

$$\lambda=8(t-1)^2(t+1)^3(t^2+3)^4(t^4+10t^2+5),$$

$$A(x)=(t^9+7t^8+8t^7+80t^6+18t^5+150t^4-64t^3+200t^2+37t+75)x^2$$
$$-(t^7+3t^6+5t^5+47t^4-13t^3+25t^2+7t+53)x+8(t-1)^2.$$

The parameter t may take any values such that the discriminant Δ_f of f does not vanish. As Δ_f factorizes as follows, t has only to avoid the value $+1$, -1 and eventual integral roots of $t^{25}+\cdots+1285335$.

$$2^{33}(t-1)^{10}(t+1)^{11}(t^2+3)^{13}(t^4+10t^2+5)^9(t^{25}+\cdots+1285335).$$

References

[1] E. V. Flynn: Large rational torsion on abelian varieties. J. Number Theory, **36**, 257–265 (1990).

[2] ——: Sequences of rational torsions on abelian varieties. Invent. Math., **106**, 433–442 (1991).

[3] B. H. Gross and D. E. Rohrich: Some results on the Mordell-Weil group of the Jacobian of the Fermat curve. Invent. Math., **44**, 201–224 (1978).

[4] J. Igusa: Arithmetic variety of moduli for genus two. Ann, of Math., **72**, 612–649 (1960).

[5] S. Kamienny: Torsion points on elliptic curves. Bull. of Amer. Math. Soc., **23**,

371–373 (1990).

[6] F. Leprévost: Famille de courbes de genre 2 munies d'une classe de diviseurs rationnels d'ordre 13. C. R. Acad. Paris, série 1, **313**, 451–454 (1991).

[7] ——: Familles de courbes de genre 2 munies d'une classe de diviseurs rationnels d'ordre 15, 17, 19 ou 21. ibid., série 1, **313**, 771–774 (1991).

[8] ——: Points rationnels de torsion de jacobiennes de certaines courbes de genre 2. ibid., série 1, **316**, 819–821 (1993).

[9] B. Mazur: Rational points of modular curves. Modular Functions of One Variable V. Lect. Notes in Math., vol. 601, Springer-Verlag, Berlin, New York, pp. 107–148 (1977).

[10] T. Shioda: Algebraic cycles on hypersurfaces in P^N. Adv. stu. in Pure Math., **10**. 717–732 (1987).

[11] A. Silverberg: Torsion points on abelian varieties of CM-type. Comp. Math., **68**, 241–249 (1988).